AFFIDAVIT

I, Jarred A. Payne, a Task Force Officer ("TFO") with the Federal Bureau of Investigation ("FBI"), being duly sworn, do hereby depose and state the following:

INTRODUCTION AND AGENT BACKGROUND

1. I have been employed as a law enforcement officer with the Kanawha County, West Virginia Sheriff's Office since February 2017. Prior to employment at the Kanawha County Sheriff's Office, I was employed as a Police Officer in West Virginia from 2009-2017. I am currently assigned to the FBI as a Task Force Officer. While assigned to the FBI, I have investigated federal criminal violations related to high technology or cybercrime, child exploitation, and child pornography. I have gained experience through training at FBI's Child Exploitation Unit, the United States Secret Service's National Computer Forensics Institute, the National White Collar Crime Center, Fox Valley Technical College, the West Virginia State Police Academy, and everyday work relating to conducting these types of investigations. I have investigated hundreds of cases involving child pornography both in the State of West Virginia and through various Federal investigations. Moreover, I am a deputized federal law enforcement officer who is engaged in enforcing federal criminal law, and I am authorized by law to request a search warrant.

2. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the examination of property— an iPad 7th generation tablet, as further described below and in Attachment A—which is currently in law enforcement possession, and the extraction from that property of electronically stored information described in Attachment B.

3. This affidavit is intended to show only that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter. The probable cause statement is based upon information of which I am personally aware as well as information that has been conveyed to me by other law enforcement officers.

IDENTIFICATION OF THE DEVICE TO BE EXAMINED

4. The property to be searched is an iPad 7th generation tablet, IMEI # 353203106599973 ("the Device"), and the electronic data extracted and preserved therefrom ("the Data").

5. The Device is presently in the possession of law enforcement in Charleston, Kanawha County, West Virginia, and maintained at the Kanawha County Sheriff's Office, 301 Virginia Street East, Charleston, WV 25301. The Device was lawfully seized from James Michael PRITT incident to arrest on October 1, 2021, for attempted sex trafficking of a minor, in violation of 18 U.S.C. § 1591(a). The Device has been maintained by law enforcement as physical evidence of the charged offense and as an item subject to a criminal forfeiture provision included in the single-count indictment against Pritt (Case No. 2:21-cr-00200). Upon information and belief, the Device has been maintained in such a manner that it is in the same condition as at the time it was seized.

6. Further, in order to prevent data loss and preserve the data from the Device, law enforcement conducted a data extraction of the phone ("the Data"); the Data has not been viewed or otherwise examined by anyone. More specifically, at the time the Device was seized, the software required to unlock the Device and extract the stored electronic information had not yet been updated to support the operating system on the Device. Typically, the tool to unlock a device must be utilized promptly; after 48 hours, the risk that the data will become inaccessible

increases substantially. Without being able to unlock a device, a search warrant to review the data cannot be executed. On approximately November 5, 2021, the software was updated to support extraction on the Device's operating system, and the Data was extracted that same day. During the time between the seizure of the Device and the extraction of the Data, the Device had to remain powered on (as the ability to readily unlock a device is reduced to nearly zero after a device has powered off) in a network isolation box to prevent its contents from being altered by any electromagnetic signals. The process of the data extraction transfers the electronic data from the device into a separate digital "container." However, this "container" holds the data in a format where it cannot be accessed or reviewed without first being processed through a forensic tool such as Cellebrite. Accordingly, the Data has been preserved for search through the extraction, but it has been maintained in a manner that has ensured the contents remained inaccessible prior to a Cellebrite forensic analysis pursuant to this requested search warrant.

7. The applied-for warrant would authorize the forensic examination of the Device and the Data for the purpose of identifying electronically stored data particularly described in Attachment B.

STATUTE UNDER INVESTIGATION

8. I am currently investigating PRITT for a violation of Title 18, United States Code, Section 1591(a) (attempted sex trafficking of a minor). I seek to search the Device and the Data to locate evidence of the criminal violation set forth above for items specified in Attachment B, incorporated herein by reference.

PROBABLE CAUSE

9. On or about Friday, October 1, 2021, a law enforcement employee was acting in an undercover capacity ("UCO"). In that role, the UCO had created a profile on the social

messaging application Kik and identified himself as being in the Jefferson, Kanawha County, West Virginia area. A person later identified as JAMES MICHAEL PRITT, who was present in a chat group joined by the UCO, sent a message to the UCO that same evening.

10. PRITT initiated contact with the UCO and said he needed to "get high" and that he had "a bunch a cash and alotta boredom." When the UCO asked what PRITT was looking for, PRITT stated "some amphetamines and some sweater meat." He later clarified he wanted "dope and pussy."

11. The UCO stated that he "might have the hookup on some puss." He told PRITT he had about 8 grams of methamphetamine and "a friend that can hook up with girls... but it's not for everybody if u know what I mean." He later clarified that the girls were "young." PRITT responded "I don't care" and later stated, "Even better matter a fact."

12. After discussing quantities and types of illegal drugs, PRITT told the UCO "I'll take 4 and a chick." The UCO said that his friend said his "girls are on deck," with one being 14 and one being 11. The UCO told PRITT the prices ($150 for one girl or $250 for both girls) and PRITT responded, "150 and how much for the go?"[1] The UCO responded that the drugs would be $250.

13. PRITT told the UCO that he had a room at the "Microcell in south charleston." This later was determined to be the Microtel Inn in South Charleston, Kanawha County, West Virginia.

14. When asked to send a picture to verify he was not law enforcement, PRITT refused to send a picture of himself but did send a picture of a pile of cash. As PRITT was

---

[1] During the conversation, PRITT referred to methamphetamine as "go."

requesting the UCO to hurry up in arriving to PRITT's hotel room, he told the UCO "Either digit[2] you sent earlier is fine" and "Let's do this."

15. The UCO stated that he was about to leave but said "he won't bring both which digit." The UCO also told PRITT, "No anal with either, full service ok... nothin rough." When the UCO asked PRITT to let him know, PRITT responded, "14 n the go."

16. The UCO told PRITT he would be to PRITT's location around 9:30 pm on October 1, 2021. The UCO said he had to reweigh the drugs because he had originally weighed out 8 grams instead of 4. The UCO told PRITT it would be "125 for go 150 for 14." He also asked PRITT "U got condoms or she need to bring one."

17. PRITT responded "An hour an that's a [baby chick emoji] some [snowflake emoji] and a tube" and then said "Deal."

18. PRITT sent another message stating, "Got a pic of [baby chick emoji]." The UCO sent a picture of the purported minor to PRITT in response. The UCO then asked again if PRITT had condoms, and PRITT responded, "Need some."

19. As they discussed the arrangements for meeting, PRITT asked, "How long do I get that's alotta $." The UCO said he would get an hour. PRITT also asked, "Does she dance or anything know what she's doing or do I have to give instructions?" The UCO told PRITT, "Instruct how u like. She's good. Just remember she's young so can't get rough."

20. PRITT also requested to see a picture of the drugs, and the UCO sent a picture of a plastic bag appearing to contain methamphetamine. PRITT said he would be right out to meet in the nearby Hardee's parking lot. PRITT was identified in the Hardee's parking lot by law

---

[2] During the conversation, PRITT referred to the minors and their ages as "digits."

enforcement and placed under arrest. PRITT dropped an iPad (the Device) that was in his hands at the time of his arrest; the Device was observed to be open to the messages with the UCO. PRITT was also in possession of $150 in United States currency.

21. PRITT gave a statement to law enforcement following his arrest. He admitted that he was aware of the age of the girl but did not intend to do anything sexual. PRITT stated that his intention was to rob the UCO of the drugs and rescue the minor child.

SPECIFICS OF SEARCH AND SEIZURE OF COMPUTER AND ELECTRONIC DEVICE SYSTEMS

22. Based upon my training and experience and information related to me by agents and others involved in the forensic examination of computers and other electronic devices, I know that data can be stored on a variety of computer systems and storage devices, including external and internal hard drives, flash drives, thumb drives, micro SD cards, macro SD cards, DVDs, gaming systems, SIM cards, cellular phones capable of storage, floppy disks, compact disks, magnetic tapes, memory cards, memory chips, and online or offsite storage servers maintained by corporations, including but not limited to "cloud" storage.

23. As is the case with most digital technology, communications by way of computer or cellular phone can be saved or stored on the computer used for these purposes. Storing this information can be intentional, i.e., by saving an e-mail as file on the computer or saving the location of one's favorite websites in, for example, "bookmarked" files. Digital information can also be retained unintentionally, e.g., traces of the path of an electronic communication may be automatically stored in many places (e.g., temporary files or ISP client software, among others). In addition to electronic communications, a computer user's Internet activities generally leave traces or "footprints" in the web cache and history files of the browser used.

24. I submit that there is probable cause to believe the items in Attachment B will be stored on the Device for at least the following reasons:

a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

b. Deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

c. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

25. As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how the Device was used, the purpose of its use, who used it, and when. There is probable cause to believe that this forensic electronic evidence will be on the Device because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the

storage medium that can reveal information such as online nicknames and passwords. Operating systems can record the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.

b. Information stored within a computer and other electronic storage media may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a computer or storage media (*e.g.*, registry information, communications, images and movies, transactional information, records of session times and durations, Internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or storage media. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence.

c. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculpating or exculpating the computer owner.

d. Moreover, information stored within a computer may provide relevant insight into the computer user's state of mind as it relates to the offense under investigation. For example, information within the computer may indicate the owner's motive and intent to commit a crime (*e.g.*, internet searches indicating criminal planning), or consciousness of guilt (*e.g.*, running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

e. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.

f. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

g. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of

counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

h. I know that when an individual uses a computer to distribute or attempt to distribute child pornography, the individual's computer will generally serve both as an instrumentality for committing the crime and also as a storage medium for evidence of the crime. The computer is an instrumentality of the crime because it is used as a means of committing the criminal offense. The computer is also likely to be a storage medium for evidence of a crime. From my training and experience, I believe that a computer used to commit a crime of this type may contain: data that is evidence of how the computer was used; data that was sent or received; notes as to how the criminal conduct was achieved; records of Internet discussions about the crime; and other records that indicate the nature of the offense.

FORENSIC ANALYSIS

26. Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the Device consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the Device to human inspection in order to determine whether it is evidence described by the warrant. If the Device has been locked using a passcode, the examination may also include the use of computer programs or other devices to bypass the passcode or otherwise access the material located on the Device.

27. *Manner of execution.* Because this warrant seeks only permission to examine a device already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

CONCLUSION

28. I submit that this affidavit supports probable cause for a search warrant authorizing the examination of the Devices described in Attachment A to seek the items described in Attachment B.

29. Moreover, I am aware that the recovery of data by a computer forensic analyst takes significant time; much the way recovery of narcotics must later be forensically evaluated in a lab, digital evidence will also undergo a similar process. For this reason, unless otherwise ordered by the Court, the return will not include the specific evidence later examined by a forensic analyst.

Further your Affiant sayeth naught.

JARRED A. PAYNE
FBI TASK FORCE OFFICER

Sworn to by the Affiant telephonically in accordance with the procedures of Rule 4.1 this 31st day of January, 2022.

DWANE L. TINSLEY
UNITED STATES MAGISTRATE JUDGE
SOUTHERN DISTRICT OF WEST VIRGINIA